APPLICATION FOR UNITED STATES PATENT

FOR

METHOD AND APPARATUS TO ADAPT THRESHOLD OF DATA FRAME PROTECT MECHANISM

INVENTORS: GINZBURG, Boris;
KONDRATIEV, Vladimir.

INTEL REFERENCE NO.: P16275
EPLC REFERENCE NO: P-5762-US

Prepared by :Moshe Vegh

Intel Corporation.

94 Em-Hamoshavot Way.
Ezorim Park, Building 2
Petach-Tikva 49527
Israel
Phone: (972) 3 9207513
Facsimile: (972) 3 9207509

METHOD AND APPARATUS TO ADAPT THRESHOLD OF DATA FRAME PROTECT MECHANISM

BACKGROUND OF THE INVENTION

[0001] In wireless local area networks (WLAN), network stations may use a channel access mechanism and a control mechanism to protect transportation of packets over the network. An example of an access mechanism may be a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and, more specifically, CSMA/CA with a binary exponential backoff method. A Request To Send/Clear To Send (RTS/CTS) mechanism is included in CSMA/CA mechanism and may be used to protect packet transportation.

[0002] For example, the activation of the RTS/CTS mechanism may be controlled by a predefined threshold, which may be referred as RTS threshold. The RTS/CTS mechanism may control packets by sending from a first station, (STA1) a RTS control message to a second station (STA2). Sending of RTS messages may be performed prior to transmission of an actual data frame, if desired. STA2 may respond with a CTS control message to STA1 and STA1 may respond by sending actual data to STA2. If STA1 does not receive the CTS message from STA2, STA1 may continue sending RTS messages to STA2 until the CTS message is received.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The subject matter regarded as the invention is particularly pointed out and distinctly claimed in the concluding portion of the specification. The invention, however, both as to organization and method of operation, together with objects, features and advantages thereof, may best be understood by reference to the following detailed description when read with the accompanied drawings in which:

[0004] FIG. 1 is a schematic illustration of a wireless communication system according to an exemplary embodiment of the present invention;

[0005] FIG. 2 is a block diagram of a station according to some exemplary embodiments of the present invention;

[0006] FIG. 3 is a block diagram of an access point according to exemplary embodiments of the present invention; and

[0007] FIG. 4 is a flowchart of a wireless communication method according to some exemplary embodiments of the present invention.

[0008] It will be appreciated that for simplicity and clarity of illustration, elements shown in the figures have not necessarily been drawn to scale. For example, the dimensions of some of the elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference numerals may be repeated among the figures to indicate corresponding or analogous elements.

DETAILED DESCRIPTION OF EMBODIMENTS OF THE INVENTION

[0009] In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However it will be understood by those of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known methods, procedures, components and circuits have not been described in detail so as not to obscure the present invention.

[0010] Some portions of the detailed description, which follow, are presented in terms of algorithms and symbolic representations of operations on data bits or binary digital signals within a computer memory. These algorithmic descriptions and representations may be the techniques used by those skilled in the data processing arts to convey the substance of their work to others skilled in the art.

[0011] Unless specifically stated otherwise, as apparent from the following discussions, it is appreciated that throughout the specification discussions utilizing terms such as "processing," "computing," "calculating," "determining," or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities within the computing system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage, transmission or display devices.

[0012] It should be understood that the present invention may be used in a variety of applications. Although the present invention is not limited in this respect, the circuits and techniques disclosed herein may be used in many apparatuses such as stations of a radio system. Stations intended to be included within the scope of the present invention include, by way of example only, wireless local area network (WLAN) stations, two-way radio stations, digital system stations, analog system stations, cellular radiotelephone stations, and the like.

[0013] Types of WLAN stations intended to be within the scope of the present invention include, although are not limited to, mobile stations, access points, stations for receiving and transmitting spread spectrum signals such as, for example, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum

(DSSS), Complementary Code Keying (CCK), Orthogonal Frequency-Division Multiplexing (OFDM) and the like.

[0014] Turning first to FIG. 1, a wireless communication system 100, for example, a WLAN communication system is shown. Although the scope of the present invention is not limited in this respect, the exemplary WLAN communication system 100 may be defined, by IEEE 802.11 -1999 standard, as a basic service set (BSS). For example, BSS may include at least one communication station, for example, an access point (AP) 110, and stations 120 130, at least one of which may be a mobile unit (MU). In some embodiments, stations 130 and 120 may transmit and/or receive one or more packets over wireless communication system 100. The packets may include data, control messages, network information, and the like. Additionally or alternatively, in other embodiments of the present invention, wireless communication system 100 may include two or more APs and two or more mobile stations. This arrangement of wireless communication system 100 may be referred by IEEE 802.11 -1999 standard as extended service set (ESS), although the scope of the present invention is not limited in this respect.

[0015] Although the scope of the present invention is not limited in this respect, AP 110 may control the communication by sending control commands of a packet protection mechanism via beacons 125, 135, 145, if desired. For example, a packet protection mechanism such as, for example, a CSMA/CA with binary exponential backoff may include a RTS/CTS mechanism that may be used to provide collision protection to the transmission of a data frame, if desired.

[0016] Turning to FIG. 2, a block diagram of a station 200 according to some exemplary embodiments of the present invention is shown. Although the scope of the present invention is not limited in this respect, station 200 may include an antenna 210, a transmitter (TX) 220, a receiver (RX) 225 and a medium access control (MAC) processor 230. In some embodiments of the invention, MAC processor 230 may include a collision estimator 240, a hidden node detector 250, an RTS threshold adapter 260, an RTS/CTS mechanism 270 and a memory 280.

[0017] Although the scope of the present invention is not limited in this respect, antenna 210 may be an omni-directional antenna, a monopole antenna, a dipole antenna, an end fed antenna, a circularly polarized antenna, a micro-strip antenna, a diversity antenna and the like. MAC processor 230 may include a digital signal processor, a communication processor, and the like.

[0018] Although the scope of the present invention is not limited in this respect, station 200 may include TX 220 and RX 225 to transmit and receive signals, respectively. If a packet 215 is received successfully, and at least a portion of the information in a received packet 217, for example, the information on channel load, if desired, may be input to collision estimator 240. In some embodiments of the invention, RTS/CTS mechanism may be used to overcome an increase in collision rate due to "a hidden node", for example, a station 140, which may be referred to herein as "hidden station. Turning back to FIG. 1, for example, stations 120, 130 and AP 110 may be referred to as "visible stations" because they may receive all transmissions from other stations. However, a hidden station, for example, station 140 may receive transmissions of one station, for example, AP 110 and may not received transmissions from other stations, e.g., stations 120 and 130.

[0019] Although the scope of the present invention is not limited in this respect, RTS\CTS mechanism 270 may be used to control the data frame transportation if for example, according to the value of a collision rate parameter, a possible hidden station, e.g., station 140, is determined to be within the wireless communication system 100. Hidden node detector 250 may detect the hidden station by monitoring the frames from the BSS stations. For example, hidden node detector 250 may detect the hidden station if a CTS message from AP 110 is received but the corresponding RTS message from station 120 is not received, and the channel is sensed as clear before the CTS message is received. Additionally or alternatively, hidden node detector 250 may detect a hidden station if an acknowledgement message from AP 110 to station 140 is received but the corresponding packet from station 120 is not received and the channel is sensed as clear before the acknowledgement message is received.

[0020] Although the scope of the present invention is not limited in this respect, hidden node decoder 250 may store in memory 280 the detected hidden station and may enable a hidden node protection. For example, in some embodiments of the invention, hidden node detector 250 may adapt a RTS threshold by sending a RTS threshold value to RTS threshold adapter 260. RTS/CTS mechanism 270 may be enabled and/or disabled according to the value of the RTS threshold. RTS/CTS mechanism 270 may protect the packet from collisions and from an increase in the network load. In some embodiments of the invention, memory 280 may include a list of hidden node stations 285. Hidden node detector 250 may add or remove stations from hidden node list 285, for example, when a visible station becomes hidden or when a hidden station becomes visible, if desired. In some embodiments when hidden node list 285 become empty, hidden node detector 250 may command RTS threshold adapter to adapt the RTS threshold value. The adaptation of the RTS threshold value may cause RTS/CTS mechanism 270 to disable the hidden node protection, if desired.

[0021] Turning to FIG. 3 a block diagram of an AP 300 according to some exemplary embodiments of the present invention is shown. Although the scope of the present invention is not limited in this respect, AP 300 may include at least one antenna 310 that may be used to transmit and/or receive data packets over wireless communication system 100 (FIG. 1), for example, WLAN. In embodiments of the invention, antenna 310 may be an omni-directional antenna, a monopole antenna, a dipole antenna, an end fed antenna, a circularly polarized antenna, a microstrip antenna, a diversity antenna and the like.

[0022] Although the scope of the present invention is not limited in this respect, AP 300 may include a transmitter (TX) 320, a receiver (RX) 325 and a MAC processor 330. TX 320 and RX 325 may be used to transmit and/or received packets over the air. Some of the packets may be included in a control signal, e.g., beacon 125. Beacon 125 may include data, control messages, network parameters such as, for example, a collision rate parameter, and the like. In some embodiments, MAC processor 330 may include a RTS/CTS mechanism 370 that may be enabled and/or disabled based on a value of an adaptable RTS threshold 385. A RTS threshold adapter 360 may adapt the value of RTS threshold 385 based on a packets collision rate. Although the scope of the present invention is not limited in this respect, RTS\CTS mechanism 370 may be enabled or disabled by comparing the value of adaptable threshold 385 to the length of the packet. For example, RTS/CTS mechanism 370 may be enabled if the length of the packet is below the adaptable threshold 385 and/or the RTS/CTS mechanism may be disabled if the length of the packet is above adaptable threshold 385.

[0023] Although the scope of the present invention is not limited in this respect, threshold adapter 360 may be included in MAC processor 330. Threshold adapter 360 may calculate the value of adaptable threshold 385 based on a collision rate parameter received from a control signal, for example, from beacon 125, if desired. Furthermore, in some embodiments, threshold adaptor 360 may calculate the value of adaptable threshold 385 based on an average collision rate, a transmission data rate and a control message packet length.

[0024] In some embodiments of the invention, MAC processor 330 may include a collision estimator 340 to estimate the average collision rate from the received collision rate parameter, and a hidden node detector 350 to detect a hidden station and by to enable the RTS/CTS mechanism 370. In this embodiment, hidden node detector 350 may receive a collision rate parameter from RX 325 and may enable the RTS/CTS the transmission 370 by reducing the value of RTS threshold 385, if desired.

[0025] Turning to FIG. 4 a flowchart of a method to adapt a threshold to select a packet control mechanism according to some exemplary embodiments of the present invention is shown. Although the scope of the present invention is not limited in this respect, the exemplary method may adapt an $\mathrm{RTS}_{\mathrm{threshold}}$ according to a collision rate in a BSS of a WLAN. In some embodiments of the present invention, the adaptation of $\mathrm{RTS}_{\mathrm{threshold}}$ may be performed according to the following equation:

$$RTS_{threshold} = T_{phy}\frac{1-c}{c} * r + \frac{L_{rts}}{c} \qquad \text{(Equation 1)}$$

wherein T_{phy} may be the physical layer (PHY) overhead (in seconds (sec));

L_{RTS} may be the RTS packet length (in bits);

r may be the current data rate (in bit/sec); and

c may be the current collision rate.

[0026] Although the scope of the present invention is not limited in this respect, use of the RTS/CTS mechanism may be controlled through the $\mathrm{RTS}_{\mathrm{threshold}}$. For example, if the packet length is greater than the $\mathrm{RTS}_{\mathrm{threshold}}$, then the RTS frame may be sent prior to the data, if desired. Let P be the transmission power, T_{RTS} the length of the RTS packet, T_{data} the length of data packet, and c the collision rate ($0 \leq c \leq 1$), in some embodiments, the power required to send a data packet with the RTS/CTS mechanism may be estimated using the following equation:

$$E_{RTS} = P \cdot \left(\frac{T_{RTS}}{1-c} + T_{data} \right) \quad \text{(Equation 2)}$$

The power required to send a data packet without the RTS/CTS mechanism may be estimated using the following equation:

$$E_{noRTS} = P \frac{T_{data}}{1-c} \quad \text{(Equation 3)}$$

[0027] Although the scope of the present invention is not limited in this respect, using the estimations of Equations 2 and 3, a condition for using RTS may be $E_{RTS} < E_{noRTS}$, which condition may be represented as follows:

$$T_{data} > \frac{T_{RTS}}{c} \quad \text{(Equation 4).}$$

In some embodiments of the invention, an air time *T* for a packet of length *L*, which may be sent at a data rate *r*, may be calculated as follows:

$$T = T_{PHY} + \frac{L}{r} \quad \text{(Equation 5)}$$

wherein T_{phy}, may be a PHY overhead time.

[0028] Although the scope of the present invention is not limited in this respect, AP 110 may receive from beacon 125 a collision rate parameter. AP 110 may collect statistics of the collision rate parameter for *N* beacon (e.g. beacon 125) periods, wherein *N* may be any suitable number (box 400). AP 110 may calculate based on the statistic the average collision rate *c* (box 410). In some embodiment of the invention, AP 110 may determine the transmission rate of the transmitted packet (boxes 420, 430). AP 110 may compare the average collision rate c with a collision rate threshold $C_{threshold}$ (decision box 440). For example, $C_{threshold}$ may be defined as follows:

$$c_{threshold} = \frac{L_{rts}}{L_{\max}} \quad \text{(Equation 6)}$$

wherein, L_{max} may represent a maximum data packet length.

[0029] Although the scope of the present invention is not limited in this respect, if the average collision parameter *c* is below $C_{threshold}$ then AP 110 may transmit the packet with a predetermined packet control mechanism other than the RTS/CTS mechanism, for example, CSMA/CA control mechanism 355 (box 470). If *c* is above $C_{threshold}$

then the length of the transmitted packet, L_{packet}, may be compared to $RTS_{threshold}$ (decision box 450).

[0030] Although the scope of the present invention is not limited in this respect, if the length of the transmitted packet L_{packet} is below RTS threshold, $RTS_{threshold}$, then AP 110 may transmit the packet with a predetermined packet control mechanism other than the RTS/CTS mechanism, for example, CSMA/CA control mechanism 355 (box 470). If the length of the transmitted packet, $L_{packet,}$ is above the RTS threshold, $RTS_{threshold,}$ then AP 110 may transmit the packet with the RTS/CTS control mechanism (box 460)

[0031] Although the scope of the present invention is not limited in this respect, it can be seen from equation 1 that $RTS_{threshold}$ may be adapted before transmitting a packet because the average packet collision parameter c may be adjusted before transmission of the packet. In box 480, AP 110 may schedule a new packet for transmission and may be initialized for transmission of the new packet (box 490). Although the scope of the present invention is not limited in this respect, the method of enabling and/or disabling the packet protection control mechanism by adapting the $RTS_{threshold}$ based on the average collision parameter *c* may be repeated for a packet transmission.

[0032] While certain features of the invention have been illustrated and described herein, many modifications, substitutions, changes, and equivalents will now occur to those skilled in the art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall within the true spirit of the invention.